DETAILED ACTION

1. Claims 1-5, 7-13, 15-20 and 22-26 are pending in this application.

2. Claims 1, 9, 16 and 23 are currently amended.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Rejections - 35 USC § 103

4. Claims 1-3, 5, 7-11, 13, 15-18, 20 and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (Patent No.: US 6,704,874 B1) and further in view of Pifer et al. (Patent No.: US 4,914,444) (hereinafter "Pifer") and Halstead, Jr. et al. (Patent No.: 5,896,524) (hereinafter "Halstead").

5. As to claim 1, Porras discloses a network security system (abstract) comprising: a first distributed software agent to collect a first stream of alerts from a first network security device having a first clock (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock (column 6, lines 13-17); a second distributed software agent comprising a processor configured to collect a second stream of alerts from a second network security device having a second clock (FIG. 1, items 12-16 referred to different networks, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the second stream representing an event detected by the

second network security device and including a time of detection by the second network security device according to the second clock (column 6, lines 13-17); and a manager module in communication with the distributed software agents, the manager module comprising a processor configured to: receive the first and second stream of alerts (FIG. 1, column 3, lines 62-67 and column 4, lines 10-26), identify a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address (column 6, lines 19-27 and column 8, lines 37-47);

Porras is silent to determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and if the first clock and the second clock are not synchronized, synchronize the first clock and the second clock; modifying a least of a timestamp within the first alert and a timestamp within the second alert; and correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule. However, Pifer discloses to determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and if the first clock and the second clock are not synchronized, synchronize the first clock and the second clock and correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule ("The central site correlates lightning events observed by two detectors based on the time interval between plural lightning events observed by the detectors" –e.g. see col. 2, lines 1-15; Applicant should note that correlating alert according to a rule and

satisfying a condition of the rule is taught by determining a time correction factor from the difference between the time of occurrence measured by one detector for a give lightning event" -e.g. see col. 2, lines 1-16 and lines 25-30; see also, col. 5, lines 49-52).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

Although Pifer discloses modifying a least of a timestamp within the first alert and a timestamp within the second alert; and correlate the first alert and the second alert according to a rule (col. 2, lines 34-41 and col. 4, lines 35-40, "event is calculated and used to correct the time of occurrence data for each"), neither Porras nor Pifer explicitly disclose modifying the timestamps within the alerts. However, Halstead discloses modifying the timestamps within the alerts (col. 3, lines 33-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras and Pifer as taught by Halstead in order to reduce amount of processor instructions since if the current timestamp of an alert and/or event falls into the allowable range no further work would be needed to identify the event.

6. As to claims 9, 16 and 23, these are rejected using the same rationale as for the rejection of claim 1.

7. As to claims 2, 10, 17 and 24, Porras discloses the network security system wherein the manager module determines a synchronization error using the time of detection including the first alert and the time of detection included in the second alert (column 6, lines 18-27 and column 8, lines 37-51). Porras doesn't explicitly disclose synchronizing the first clock and the second clock and correcting the synchronization error. However, Pifer discloses synchronizing the first clock and the second clock and correcting the synchronization error (abstract, lines 25-26; col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Furthermore, Pifer discloses determines a synchronization error using the time of detection including the first alert and the time of detection included in the second alert (abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

8. As to claims 3, 11 and 18, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock. However, Pifer discloses synchronizing the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock (col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to

modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

9. As to claims 5, 13 and 20, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock. However, Pifer discloses synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock (col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

10. As to claims 7, 15 and 22, Porras discloses the network security system wherein the second alert is corroborative of the first alert (column 6, lines 13-27 and column 8, lines 37-51).

11. As to claim 8, Porras discloses the network security system wherein the first network security device comprises an Intrusion Detection System (IDS) (column 2, lines 18-38).

12. As to claim 25, Porras discloses further comprising causing the event represented by the first alert to occur (column 2, lines 18-38).

13. As to claim 26, Porras discloses further comprising causing the event represented by the second alert to occur (column 2, lines 18-38).

14. Claims 4, 12 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras in view of Pifer, Halstead and Apel et al. (Patent No.: US 6,760,687 B2), hereinafter Apel.

15. As to claims 4, 12 and 19, neither Porras and Pifer nor Halstead explicitly discloses wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock. However, Apel disclose wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock (column 9, lines 8-15 and lines 60-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras, Pifer and Halstead by selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock as taught by Apel in order to provide a highly accurate and flexible system.

16. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

17. Applicant has amended claims 1,9,16 and 23, please see rejection above. Applicant's arguments filed August 18, 2008 have been fully considered but they are not persuasive.

Applicant argues that: "Pifer does not disclose, teach or suggest the element 'if the first and the second clock are not synchronized....correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule'."

Examiner maintains that: Pifer discloses if the first and the second clock are not synchronized....correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule ("The central site correlates lightning events observed by two detectors based

on the time interval between plural lightning events observed by the detectors" –e.g. see col. 2, lines 1-15; Applicant should note that correlating alert according to a rule and satisfying a condition of the rule is taught by determining a time correction factor from the difference between the time of occurrence measured by one detector for a give lightning event" -e.g. see col. 2, lines 1-16 and lines 25-30; see also, col. 5, lines 49-52).

Applicant argues that: "Halstead does not disclose, teach, or suggest the claimed element "if the first and the second clock are not synchronized….correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule'."

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Furthermore, Pifer discloses if the first and the second clock are not synchronized….correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule ("The central site correlates lightning events observed by two detectors based on the time interval between plural lightning events observed by the detectors" –e.g. see col. 2, lines 1-15; Applicant should note that correlating alert according to a rule and satisfying a condition of the rule is taught by determining a time correction factor from

the difference between the time of occurrence measured by one detector for a give lightning event" -e.g. see col. 2, lines 1-16 and lines 25-30; see also, col. 5, lines 49-52).

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2435